13th ICCRTS

Title: **Towards a (Preliminary) Theory of Cyberpower**

Track: C2 Concepts, Theory, and Policy

Franklin D. Kramer, Stuart H. Starr (Point of Contact), Larry K. Wentz
Center for Technology and National Security Policy (CTNSP)
National Defense University (NDU)
Grant Hall, Fort Lesley J. McNair
Washington, DC 20319

Franklin D. Kramer: 202-685-3578; KramerF@ndu.edu
Stuart H. Starr: 202-685-2657; StarrS@ndu.edu
Larry Wentz: 202-685-3914; WentzL@ndu.edu

Acknowledgments: The authors of this paper drew extensively from the inputs of several key individuals including Dan Kuehl, Greg Rattray, Ed Skoudis, Eli Zimet, Tim Thomas, Hal Kwalwasser, Tom Wingfield, Catherine Theohary, and Csaba Kalmar. We are greatly indebted to them for their contributions; however, any errors are the responsibility of the authors.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Towards a (Preliminary) Theory of Cyberpower	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
National Defense University (NDU),Center for Technology and National Security Policy (CTNSP),Grant Hall, Fort Lesley J. McNair,Washington,DC,20319	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

13th International Command and Control Research and Technology Symposia (ICCRTS 2008), 17-19 Jun 2008, Seattle, WA

14. ABSTRACT

In the 2006 Quadrennial Defense Review, a request was made to have the Center for Technology and National Security Policy (CTNSP), National Defense University (NDU) develop a theory of cyberpower. It was noted that there was a need to develop a holistic framework that would enable policy makers to address cyber issues in proper perspective. To satisfy that tasking, CTNSP convened five workshops, drawing on experts from government, industry, academia, and think tanks. Those workshops addressed a broad set of issues related to the evolution of cyberspace, cyberpower, cyberstrategy, and institutional factors that influence those factors (e.g., governance, legal issues). To develop the desired theory, this paper systematically addresses five key areas. First, the paper defines the key terms that are associated with cyberpower. Particular emphasis is placed on the terms ?cyberspace?, ?cyberpower?, and ?cyberstrategy?. Second, the paper categorizes the elements, constituent parts, and factors that yield a framework for thinking about cyberpower. Third, the paper explains the major factors that are driving the evolution of cyberspace and cyberpower. To support that effort, the paper presents strawman principles that characterize major trends. Fourth, the paper connects the various elements of cyberstrategy so that a policy maker can place issues in proper context. Finally, the theory anticipates key changes in cyberspace that are likely to affect decision making. In view of the dramatic changes that are taking place in cyberspace, it is important to stress that this effort must be regarded as a preliminary effort. It is expected that the theory will continue to evolve as key technical, social, and informational trends begin to stabilize.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**51**	

Towards a (Preliminary) Theory of Cyberpower

Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz
CTNSP, NDU

Abstract

In the 2006 Quadrennial Defense Review, a request was made to have the Center for Technology and National Security Policy (CTNSP), National Defense University (NDU), develop a theory of cyberpower. It was noted that there was a need to develop a holistic framework that would enable policy makers to address cyber issues in proper perspective.

To satisfy that tasking, CTNSP convened five workshops, drawing on experts from government, industry, academia, and think tanks. Those workshops addressed a broad set of issues related to the evolution of cyberspace, cyberpower, cyberstrategy, and institutional factors that influence those factors (e.g., governance, legal issues).

To develop the desired theory, this paper systematically addresses five key areas. First, the paper *defines* the key terms that are associated with cyberpower. Particular emphasis is placed on the terms "cyberspace", "cyberpower", and "cyberstrategy". Second, the paper *categorizes* the elements, constituent parts, and factors that yield a framework for thinking about cyberpower. Third, the paper *explains* the major factors that are driving the evolution of cyberspace and cyberpower. To support that effort, the paper presents strawman principles that characterize major trends. Fourth, the paper *connects* the various elements of cyberstrategy so that a policy maker can place issues in proper context. Finally, the theory *anticipates* key changes in cyberspace that are likely to affect decision making.

In view of the dramatic changes that are taking place in cyberspace, it is important to stress that this effort must be regarded as a preliminary effort. It is expected that the theory will continue to evolve as key technical, social, and informational trends begin to stabilize.

I. Introduction

This paper represents a preliminary effort to develop a theory of cyberpower. The chapter begins by characterizing the Terms of Reference (ToR) for the study. We then characterize the components of a "theory of cyberpower". Consistent with that characterization, we identify key terms and put forth strawman definitions of those terms. We then present a holistic framework to characterize and discuss key categories. Subsequently, we discuss theoretical dimensions of the key categories: cyberspace, cyberpower, cyberstrategy, and institutional factors. In addition, we discuss the challenges associated with connecting across these categories. The paper is supported by six appendices. These appendices include timelines of key cyber events (Appendix A), a summary of major policy recommendations to deal with terrorist threats (Appendix B), an elaboration on cyber Measures of Merit (MoMs) (Appendix C), a discussion of future cyber research initiatives (Appendix D), an enumeration of abbreviations and acronyms (Appendix E), and a list of references (Appendix F).

A. Terms of Reference

In the 2006 Quadrennial Defense Review (QDR) (Reference 1), requests were made to develop theories of space power and cyber power. The Institute for National

Strategic Studies (INSS), NDU, was tasked with developing the theory of space power (Reference 2) and the Center for Technology and National Security Policy (CTNSP), NDU, was tasked with developing the theory of cyber power.

As stated in the ToR for the cyber power task (Reference 3), "… there is a compelling need for a comprehensive, robust and articulate cyber power theory that describes, explains and predicts how our nation should best use cyber power in support of US national and security interests".

Consistent with that broad goal, the ToR identified four specific areas that the theory should account for:

- "The nation's increased use of and reliance upon national security, civil and commercial cyber capabilities;
- Other nations' and non-governmental actors' use of cyberspace;
- Direct challenges to the US's use of cyberspace; and
- The changed and projected geo-strategic environment."

B. Components of a Theory

As noted in Reference 4, a theory of warfare should address five key issues. First, it should introduce and **define** the key terms that provide the foundation of the theory. Second, it should give structure to the discussion by **categorizing** the key elements of the theory. Third, it should **explain** the elements in these categories by summarizing relevant events and introducing key frameworks or models. Fourth, it should seek to **anticipate** key trends and activities so that policy can be germane and useful. Finally, it should **connect** the various elements of the subject so that key issues can be treated comprehensively.

This theoretical framework for a theory raises one immediate issue. In the ToR it identified the need to predict, rather than anticipate, key activities. However, as described below, the cyber problem is in the midst of explosive, exponential change. In the midst of this exceptional uncertainty, it is infeasible to make reliable predictions. Thus, we have adopted the less challenging task of "anticipating" key trends and activities.

Finally, it is important to stress the following caveat: since this is a preliminary effort to develop a theory of cyberpower, the emerging theory will **not** be complete.

To highlight the challenges facing the "cyber theorist", consider the following. The cyberspace of today has its roots back in the 1970s when the Internet was conceived by engineers sponsored by ARPA. Detailed analysis of cyberspace issues often requires even broader cross-disciplinary knowledge and skills than physics. These include, *inter alia*, computer scientists, military theorists, economists, and lawyers. Each of these disciplines has its own vocabulary and body of knowledge. Thus, it is quite challenging for these stakeholders to communicate effectively. This is manifested in debates about the most basic of terms (e.g., "cyberspace") where key definitions are still contentious. Consistent with the heterogeneous nature of the problem, it is not surprising that prior efforts to characterize this space have not been successful. At present, there is no agreed upon taxonomy to support a comprehensive theory.

C. Scope

The scope of this paper is restricted in two key dimensions. First, we will restrict attention to the national security domain. Changes in cyberspace are having a major impact on social, cultural, and economic issues, but we will not address them explicitly. Second, we will limit attention to the key cyberpower issues that are confronting the

national security policy maker. Thus, there is no attempt to generate a comprehensive theory of cyberpower that touches on broader issues.

D. Approach

In order to generate this preliminary theory orf cyberpower, we have employed the following approach. First, we drew insights from observations of cyber events, experiments, and trends. Timelines for key cyber events that we have employed in developing the theory are summarized in Appendix A. Second, we built on prior national security methods, frameworks, theories, tools, data, and studies, which were germane to the problem. Finally, we formulated and hypothesized new methods, frameworks, theories, and tools to deal with unexplained trends and issues.

We implemented this approach through a series of workshops that drew upon world-leaders in the areas of interest. This included representatives from government, industry, academia, and think tanks.

Based on these inputs, we have adopted the holistic cyber framework depicted in Figure 1. This framework is patterned after the triangular framework that the military operations research community has employed to decompose the dimensions of traditional warfare. In that framework, the base consists of systems models, upon which rests more complex, higher orders of interactions (e.g., engagements, tactical operations, campaigns). Historically, the outputs from the lower levels provide the feedback to the higher levels of the triangle.

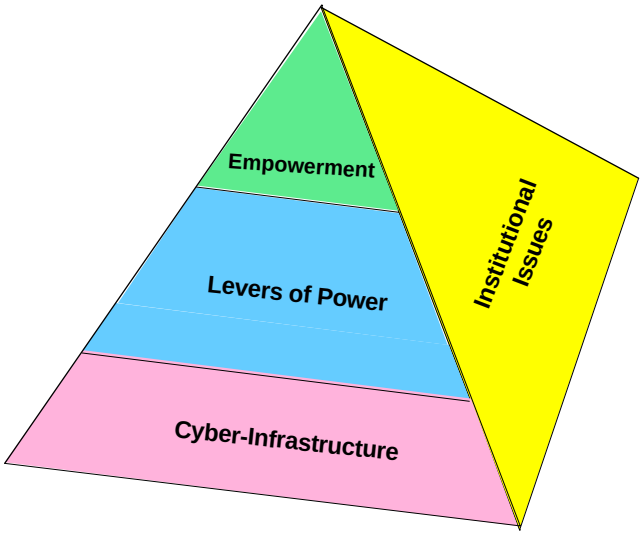


Figure 1. Broad Conceptual Framework

By analogy, the bottom of the pyramid consists of the components, systems, and systems-of-systems that comprise the cyber-infrastructure. The output from this cyber-infrastructure enhances the traditional levers of power: political/diplomatic, informational, military and economic (P/DIME). These levers of power, in turn, provide the basis for empowerment of the entities at the top of the pyramid. These entities

include, *inter alia*, individuals, terrorists, trans-national criminals, corporations, nation states, and international organizations. Note that while nation states have access to all of these levers of power, the other entities generally have access to only a sub-set of them. In addition, initiatives, such as deterrence and treaties, may provide the basis for limiting the empowerment of key entities.

The pyramid suggests that each of these levels is affected by institutional issues. These include factors such as governance, legal considerations, regulation, sharing of information, and consideration of civil liberties.

It must be emphasized that this framework is merely one of many frameworks that could be constructed to conceptualize the cyber domain. However, it has proven useful for us in decomposing the problem and developing subordinate frameworks to address key cyber issues.

E. Key Definitions

As noted above, there is a continuing discussion about the appropriate definitions for key cyber terms. For example, in their study of the "Convergence of Sea Power and Cyber Power" (Reference 6), the Strategic Studies Group (SSG), Newport, RI, identified 28 candidate definitions of the term "cyberspace". In order to categorize and compare those terms, the SSG introduced a two-dimensional space that featured the axes "focus" (present day versus future) and "centricity" (technology versus human). They observed that the definition posed by William Gibson, in his 1984 book "Neuromancer" (Reference 7), fell in the upper right quadrant of this space (e.g., futurist with some consideration of the human dimension): "A consensual hallucination… A graphic representation of data abstracted from banks of every computer in the human system."

For the purposes of this theory, we have adopted a variant of the formal definition of cyberspace that the Joint Staff employed in the National Military Strategy – Cyberspace Operations (NMS-CO) (Reference 8): "An operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and internetted information systems and their associated infrastructures". This definition does not explicitly deal with the information and cognitive dimensions of the problem. To deal with those aspects explicitly, we have introduced two complementary terms: cyberpower and cyberstrategy.

We have adopted the following definition for the term "Cyberpower". It is "the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power." In this context, the instruments of power include the elements of the P/DIME paradigm. For the purposes of this preliminary theory, primary emphasis will be place on the military and informational levers of power.

Similarly, the term "Cyberstrategy" is defined as "the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power." Thus, one of the key issues associated with cyberstrategy deals with the challenge of devising "tailored deterrence" to affect the behavior of the key entities empowered by developments in cyberspace.

Consistent with our definitions, the elements of the holistic framework can be recast as depicted in Figure 2.

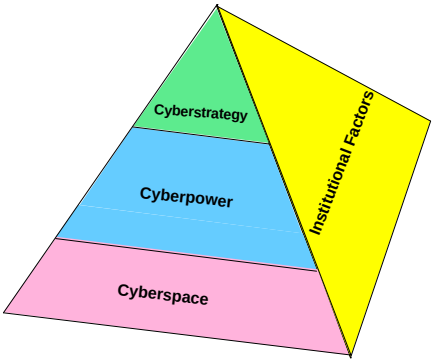


Figure 2. Cyberspace, Cyberpower, and Cyberstrategy

II. Theoretical Aspects of Cyberspace

This section begins by providing contextual material about the growth of cyberspace. It then discusses trends in cyberspace components and systems. It concludes by providing selected cyberspace "rules of thumb" and principles.

A. Context

The most remarkable aspect of the Internet has been the exponential growth in users, world-wide. Figure 3 illustrates that growth over a thirty-three year period. It can be seen that the user population increased from approximately 1M users in 1992 to 1,200M users in 2007. It is projected that the Internet will have 2B users by 2010. This number is projected to grow substantially if the One Laptop Per Child (OLPC) project is brought to fruition. That project aims to get many millions of low-cost laptops in the hands of children in under-developed countries.

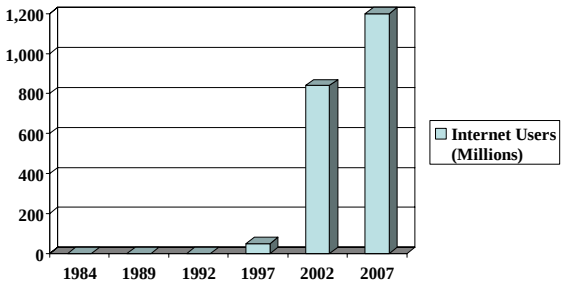


Figure 3. Number of Internet Users (Millions)

The SSG Report (Reference 6) depicted this growth from another perspective. They used 50M users as a benchmark for penetration of a mass medium. That level was achieved by radio in 38 years, television in 13 years, and the Internet in 6 years

(beginning with the introduction of the World Wide Web).

B. Cyberspace Components, Systems

From a theoretical perspective, the physics of the hardware that supports cyberspace has a significant impact on its performance. This is particularly manifested in the design of microprocessors and hard drives.

B.1 Microprocessors. Clock cycles of modern microprocessors exceed 2 GHz. Therefore, under ideal circumstances, electrons can move a maximum of 0.15 meters in a single processor clock cycle, nearing the size of the chip itself. With clock cycles going even higher[1], electronic signals cannot propagate across a chip within one clock cycle, implying elements of the chip cannot communicate with other elements on the other side of the same chip. Thus, this limitation maximizes the effective size of a single integrated microprocessor running at high clock speeds. Addressing this limitation is one of the reasons that various processor manufacturers have moved chip architectures toward multi-core processors, where multiple, semi-independent processors are etched on a single chip. Current chips have up to eight cores with substantial increases expected for the future.

B.2 Hard Drives. Figure 4 depicts computer hard drive storage capability (in gigabits per square centimeter) over the last twenty five years. It is notable that the improvement in memory was negligible for the first twenty years until IBM engineers applied the phenomenon of giant magnetoresistance[2]. Currently, improvements in memory are manifesting exponential improvement, making it feasible to create very portable devices, such as iPods, with extremely high storage capability.

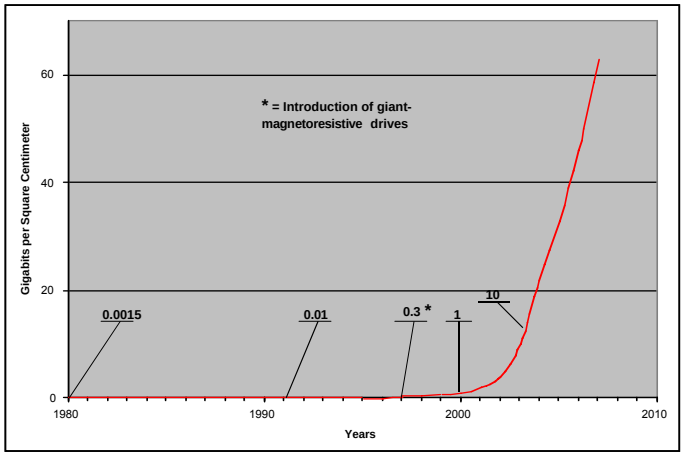


Figure 4. Hard Drive Capacity

[1] The current, fastest super computer, Lawrence Livermore's Blue Gene/L system, is capable of performing 478 trillion floating point operations per second.

[2] The Nobel Prize in Physics for 2007 was awarded to Albert Fert and Peter Grunberg, who independently discovered this phenomenon.

These two examples suggest that a careful technology assessment is needed to assess if and when bottlenecks in technology will be overcome that limit current performance.

B.3 Systems. The military community has embraced the underlying computer science principles associated with the Internet, although they have enhanced security for classified systems by developing "air gapped" networks (e.g., SIPRnet, JWICS). Figure 5 provides a cartoon of that implementation for the notional Global Information Grid (GIG).

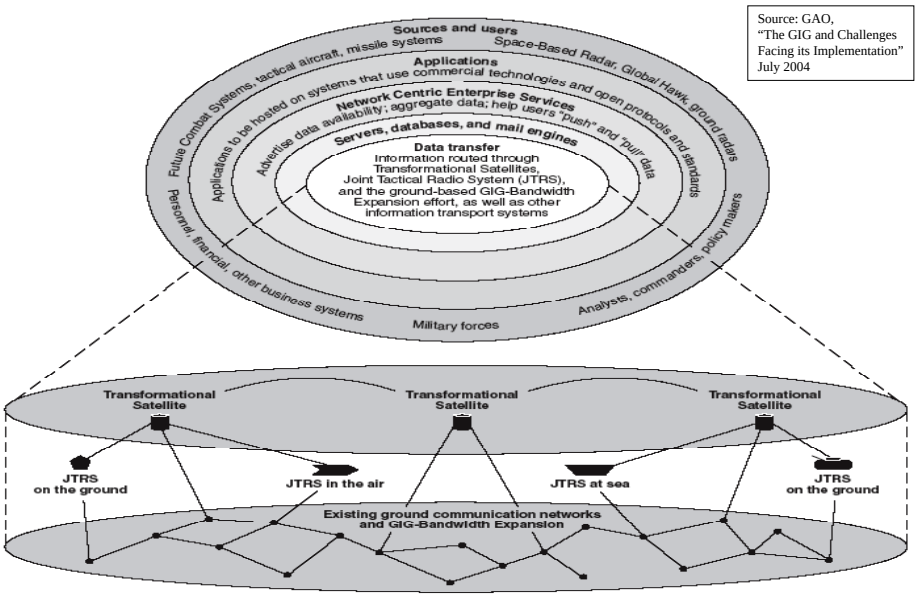


Figure 5. A Framework to Characterize the GIG

There are several distinctive aspects of the evolving GIG. First, for the transport layer, the plan is to employ a heterogeneous mix of satellite (e.g., Transformational Satellites), airborne (e.g., selected Joint Tactical Radio Systems (JTRS)), and surface (e.g., fiber optic) telecommunications media. As a side note, the military is finding it difficult to develop many of these elements within acceptable levels of performance, schedule, and cost.

Second, there is interest in employing a Service Oriented Architecture (SOA) to provide loose coupling among key systems. Third, they have developed Communities of Interest to address the challenges associated with the data that will flow through the systems (e.g., specify meta-data; deal with issues of pedigree). It has been articulated that they wish to transition from the principle of "need to know" to "need to share". Finally, they hope to assimilate the Services' visions of future systems into the GIG (e.g., USA LandWarNet; USN ForceNet; USAF C2 Constellation).

In order to achieve this vision it will require the concerted efforts of the military's system-of-systems engineers. Reference 8 identifies the many challenges that must be addressed to achieve this vision.

C. Cyberspace "Rules of Thumb", Principles

To help explain the various trends in cyberspace, one can provide several "rules of thumb" and strawman "principles". Several "rules of thumb" are employed in the community which are incorrectly characterized as "laws". For example Moore's "Law" indicates that the number of transistors on a chip approximately doubles every 18 months (Reference 9). This has contributed to the production of devices that have enhanced computational power and decreased size. Although this trend is generally representative of past behavior, there is concern that it may be extremely difficult to sustain that trend in the indefinite future without a fundamental, expensive change in the underlying technology (e.g., transition to nanotechnology). Second, as noted above in Figure 6, recent break-throughs in physics have put the growth in hard drive capacity on an exponential curve, vice a conservative linear curve. Ultimately, this curve will reach a level of saturation (i.e., an "S-curve") that is representative of a mature technology. Lastly, the current limitation in Internet Protocol (IP) addresses (i.e., 32 bits) will be dramatically overcome once the transition to IPv6 is implemented and 128 bits are available for IP addresses.

Based on the authors' deductions, several strawman cyberspace "principles" can be articulated. First, the offensive has the advantage. This is due, in part, to the "target rich" environment that an adversary faces. This makes it difficult for the defense to prioritize and defend selected targets. In addition, the existing architecture makes it very challenging to attribute an attack if an adversary seeks to be anonymous. If cyberspace is to be more resistant to attack, it will require a new architecture that has "designed in" security. However, it will be a challenge to transition, effectively and efficiently, from the current legacy system to a more secure objective system.

To anticipate key changes in cyberspace, we have identified several key trends. However, it is extremely difficult to provide quantitative estimates as to how rapidly these trends will be manifested. Thus, the following should be regarded as a partial, qualitative list of some of the most significant potential changes.

First, there is an increased move to adoption of IP-based systems. As a consequence, one can anticipate a convergence of telephone, radio, television, and the Internet. As one example, there is a dramatic use of Voice over IP (VoIP) (with attendant security issues) in the area of telephony. Second, we are seeing the emergence of sensor networks that feature an extremely large number of heterogeneous sensors. As one manifestation, we are seeing the netting of extremely large number of video cameras in urban areas, raising issues in the civil liberties community. Third, we are seeing an inexorable trend towards proliferation of broadband and wireless. An example of this trend was the plan to have city-wide deployment of Worldwide Interoperability for Microwave Access (WiMax). However, this trend suggests the difficulty in predicting when a trend becomes a reality. Nextel had made this objective the key to their strategy; however, they have recently observed that the technology has not matured sufficiently to implement it in the near-term (Reference 10). Fourth, we are observing enhanced search capabilities, both for local systems and the entire Internet. One of the keys to this trend has been industrial competition to develop improved search engines (in part, to enhance advertising revenue). Fifth, we are seeing extraordinary efforts to enhance human/machine connectivity. As one example, we are seeing direct nerve and brain connections to computers or prostheses, arising from efforts to treat soldiers injured by improvised

explosive devices (IEDs) in Iraq. Finally, we are seeing dramatic increases in user participation in information content. This trend is manifested through the proliferation of blogs, contributions to wikis, participation in social networks (e.g., MySpace, FaceBook), and involvement in virtual reality environments (e.g., Second Life).

III. Theoretical Aspects of Cyberpower

This section begins by analyzing environmental theories of power and extending these results to cyberpower. It then provides selected frameworks which are useful for conceptualizing cyberpower. These include frameworks for Net-Centric Warfare (NCW) and influence operations. The section concludes by citing several cyberpower rules of thumb and principles.

A. Environmental Theories of Power

In the discussions that led to this study, it was observed that the theories of Mahan played a major role in shaping the US perspectives and strategies on naval power. It was suggested that cyberpower needed a comparable perspective to shape its strategy in cyberspace.

Consistent with that interest, we have re-evaluated the various environmental theories of power. These included analyses of land power (Mackinder), naval power (Mahan), airpower (Douhet), and space power (Gray and Sloan). Based on these analyses, four common features of environmental power theories were identified: technological advances; speed and scope of operations; control of key features; and national mobilization.

Consistent with each of these features, the following implications were drawn for a theory of cyberpower. With respect to technological advances, it was observed that dependency on cyberspace has given rise to new strategic vulnerabilities. This vulnerability has been dramatized by the specter of a “cyber Pearl Harbor” and the realization that the existing cyberspace is vulnerable to a variety of adversary attacks (e.g., denial of service attacks; exfiltration of sensitive but unclassified information; potential corruption of sensitive data). In addition, due to the diffusion of low cost cyberspace technology, the power of non-states (e.g., individuals, terrorists, transnational criminals, corporations) has been greatly enhanced (see below).

Improvements in cyberspace have also served to enhance the speed and scope of operations. This is manifested in the speed at which global operations can be conducted (e.g., the ability to successfully engage time sensitive targets, any where in the world). In addition, it has led to improvements in the ability to automate command and control, dramatically decreasing the classic Observe-Orient-Decide-Act (OODA) loop process.

In the environmental theories of power, emphasis was placed on controlling key features. For example, in naval theories this entailed the control of key “choke points” (e.g., the Straits of Malacca), while in space power, there was interest in controlling key geosynchronous orbit locations. In the case of cyberspace, the key features of interest are man-made. Thus, for example, there is interest in defending “cyber hotels” where key information and communications systems are concentrated. In addition, while the choke points in the physical world tend to be immutable, they may change relatively rapidly in cyberspace (e.g., location of extensive server farms).

Finally, national mobilization is a key measure of cyberpower. To ensure that it is available when needed, it is vital to ensure that the US has access to a cadre of

cyberspace professionals. This argues for re-examining career progression for cyberspace professionals in the military Services. In addition, it is important to establish links to the private sector where the bulk of cyberspace professionals reside. This suggests that a reserve reservoir should be established to provide access to this intellectual capital in the event of national need.

B. Net-Centric Warfare

Work is needed to enhance and apply the existing conceptual framework for NCW. As illustrated in Figure 6, the NCW process involves consideration of the interactions among the physical, information, cognitive, and social domains. There is a need to develop better analytic tools for all aspects of this process, particularly in the cognitive and social domains. One potential source of intellectual capital is the forthcoming initiative to improve human, behavior, social, and cultural (HBSC) models and simulations. This issue is discussed later in this chapter.

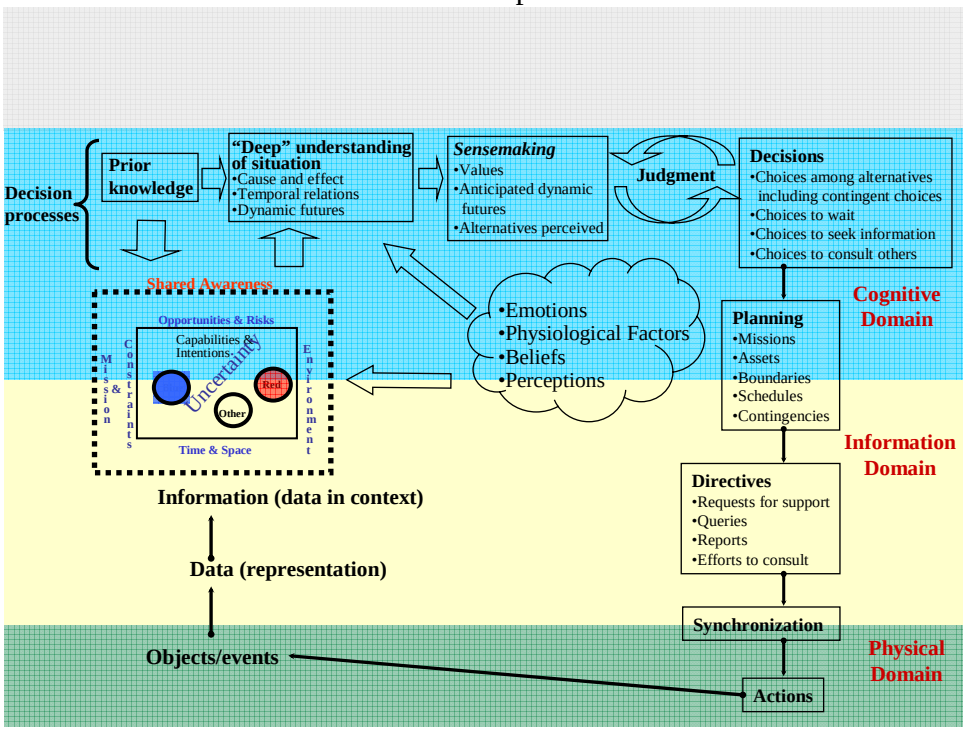


Figure 6. Conceptual Framework for NCW

We observe that the US Government (USG) has tended to focus on the opportunities offered by changes in cyberspace, rather than the risks that we are assuming. To summarize that dichotomy, Table 1 identifies the opportunities and risks associated with military activities at the strategic, operational, and tactical levels.

Level	Opportunities	Risks
Strategic	• NCW-enabled • New "Center of Gravity" opportunities (e.g., deterrence; "virtual conflict")	• Loss of technical advantage • Rapidly changing operating environment • Military dependence on key systems (e.g., GIG)
Operational	• Phasing of operations • Enhanced force structure mix (e.g., cheaper, more precise)	• Loss of advantage in operational pace
Tactical	• Discover and track adversaries using cyberspace	• New front for adversaries to build resources

Table 1. Military Opportunities & Risks in Cyberspace

As can be seen in Table 1, the risks at the strategic level include loss of technical advantage (due to the diffusion of cyberspace technology), potential rapid change in the operating environment (e.g., possibility that nations such as China could "leap-frog" the US by transitioning rapidly to IPv6), and the vulnerabilities associated with military dependence on key systems (e.g., the GIG). At the operational level, the diffusion of cyberspace technology could result in the US loss of advantage in operational pace. Finally, at the tactical level, advances in cyberspace could generate a new front for adversaries to build resources. These observations suggest that the USG might be assuming significant, unknown risks by failing to take a balanced perspective of key cyberspace trends. It also implies the need to undertake more extensive risk assessments to understand the potential "down-side" of key dependencies.

To begin to deal with these risks, steps should be taken at the strategic, operational, and programmatic levels. At the strategic level, steps should be taken to ensure the resilience of supporting critical infrastructures (e.g., electric power generation and transmission). At the operational level, it is vital to plan to conduct operations against an adversary that is highly cyberwar-capable. This should include the creation of a highly-capable Opposing Force (OPFOR) that would be employed extensively in experiments and exercises. Finally, at the programmatic level, emphasis should be placed on addressing cyberspace implications in the development process. This should include placing higher priority on the challenges of Information Assurance. Overall, an improved analytic capability is required to address each of these issues.

C. Influence Operations

A strawman framework has been developed to help the community plan for and implement influence operations (Figure 7). This framework represents an extension of the Mission Oriented Approach to Command and Control (C2) that was developed and applied to a variety of C2 issues in the 1980s (Reference 11).

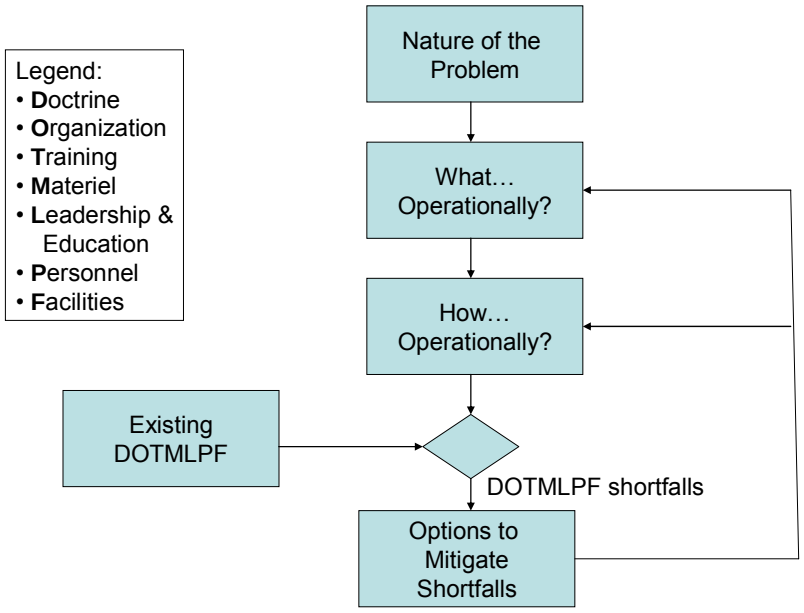


Figure 7. Strawman Framework for Analyzing Influence Operations

This approach begins with the articulation of the nature of the problem of interest. It then poses a sequence of questions. First, what is the operational objective of the operation? As noted in the case study in Reference 12, a reasonable objective may be to establish a trust relationship with the indigenous population (vice "winning their hearts and minds"). Second, how should this operational objective be accomplished? Again, as noted in Reference 12, a decision was made to work with surrogate audiences in order to reach the undecided population. These surrogate audiences included the local media, religious leaders, educational leaders, political leaders, and tribal leaders. Consistent with those surrogate audiences, organizations and processes were established to reach out to them effectively. At this point, one can characterize the existing Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF) activities and compare them to the operational needs. This will give rise to DOTMLPF shortfalls and the articulation of options to mitigate them. It may also prompt the operator to re-evaluate the operational goals and the operational activities to support them.

This process should be refined and applied to a broader variety of strategic, operation, and tactical influence operations. In particular, it can be used to explore the utility of employing new options in cyberspace to improve future influence operations.

D. Cyberpower "Rules of Thumb", Principles

One of the so-called "laws of cyberpower" was formulated by Bob Metcalfe. He postulated that the value of a telecommunications network is proportional to the square of the number of users of the system (n^2) (Reference 13). However, there is no empirical data to support this "law". In a recent article (Reference 14), it is observed that the value is closer to nlog(n).

From an analytical perspective, the former Office of Force Transformation has supported a number of studies to relate the impact of net-centricity on enhancements in

cyberpower (primarily in the military domain). These on-going studies have demonstrated that net-centricity can have a substantial affect on mission effectiveness for selected mission areas. For example, the use of Link 16 by aircraft in airborne combat can enhance air-to-air loss exchange ratios by approximately 2.5 (Reference 15). However, the complexity of modern conflict is such that it is difficult to assess the affect of net-centricity on complex missions (e.g., air-land operations; stability and reconstruction operations). This suggests that additional experiments will be needed to assess the quantitative value of net-centricity for complex missions, in which better control is exercised over potentially confounding variables.

IV. Theoretical Aspects of Cyberstrategy

We have identified an extensive list of entities that are being empowered by changes in cyberspace. This list includes individuals, hacktivists[3], non-governmental organizations (e.g., Red Cross), terrorists, trans-national criminals, corporations, nation-states, and international governmental organizations (e.g., the United Nations). This section focuses on two of these entities: terrorists and selected nation states. It then briefly discusses the challenges associated with cyber deterrence. The section concludes by citing selected cyberstrategy "rules of thumb" and principles.

A. Terrorists

Several sources have observed that terrorists are being empowered by changes in cyberspace (Reference 16). With the loss of physical sanctuary in key areas (e.g., Afghanistan), they have been turning to the sanctuary of cyberspace to perform a variety of key, inter-related functions. These functions include, *inter alia*, recruiting of malleable candidates, raising resources to support their operations, planning their operations (employing such open-source tools as Google Earth), commanding and controlling their operations, conducting influence operations (e.g., disseminating their perspectives of operations in Iraq to sympathetic and uncommitted audiences), and educating and training supporters on a variety of subjects (e.g., interpretations of the Koran; building and deploying IEDs).

Terrorists have found cyberspace to be an attractive milieu for several reasons. First, the cost of entry is low. One can acquire the latest cyber technology for hundreds-to-thousands of dollars and exploit key open-source software. In addition, terrorists can take full advantage of the extraordinary sums that have been invested by the commercial sector in cyber infrastructure (including communications and navigation systems). Second, cyberpace provides rapid, world-wide reach. Thus, they are able to transcend the limited geographic reach of their prior physical sanctuary and perform the key functions cited above. Third, there is concern that terrorists are developing linkages with trans-national criminals to support their objectives. The trans-national criminals are able to provide terrorists with cyber knowledge while profiting from the relationship.

Recently, a number of reports have been issued that suggest strategies for the USG to pursue to counter the terrorists use of cyberspace. As a point of departure, the results of one Blue Ribbon study group are summarized in Appendix B (Reference 17).

---

[3] Wikipedia definition: Hacktivism (a portmanteau of hack and activism) is often understood as the writing of code, or otherwise manipulating bits, to promote political ideology…

B. Nation States

From a nation-state perspective, different combinations of levers of power are employed to generate desired effects. From a theoretical perspective, these nations formulate their strategy though a mix of P/DIME activities. The effects of these activities are manifested in Political, Military, Economic, Social, Information, and Infrastructure (PMESII) areas.

Using the PMESII paradigm, one can begin to characterize how cyber changes have empowered the US. In the political dimension, changes in cyberspace have encouraged democratic participation by the population. With respect to the Internet, it has provided a forum for the individual to articulate his views (e.g., proliferation of blogs, contributions to wikis). In addition, political candidates are finding the Internet to be a useful vehicle for raising resources from grass root supporters. Furthermore, Internet sites such as YouTube have enhanced the accountability of candidates.

In the military dimension, the concept of NCW has enhanced effectiveness in selected operational domains (e.g., air-to-air combat). Efforts are still required to quantify the military benefits that are achievable for more complex military operations (e.g., air-land maneuver).

Economically, the commercial sector has seen dramatic improvements in industrial productivity (e.g., Boeing's use of computer aided design tools to support the development of the 777 aircraft and the more recent development of the 787). These cyber-based advancements are giving rise to considerable improvements in responsiveness (e.g., time to market) and cost reductions (e.g., outsourcing "back-room operations" to other nations).

Socially, the development of cyberspace has increased social interactions is several ways. Tens of millions of users participate in social networking sites (e.g., MySpace, FaceBook). In addition, millions of users, world-wide, participate in virtual reality environments (e.g., Second Life). In fact, it has been rumored that terrorist organizations are using virtual reality environments to explore proto-typical operations.

In the information dimension, the Internet has increased dissemination of information, world-wide. Given the US' strong position in entertainment (movies, games) and advertising, it is argued that it provides a strong forum for promoting "soft power" (Reference 18).

Finally in the infrastructure dimension, many critical infrastructures have been using the Internet to facilitate more efficient and effective operations. However, this constitutes a "double edged sword" because of the potential vulnerability of Supervisory Control and Data Acquisition (SCADA) systems.

Overall, it must be stressed that empowerment is more than the sum of the individual PMESII factors.

Conversely, many near-peers tend to employ other concepts for cyberstrategy. For example, Chinese writings on the subject focus on stratagems, objective and subjective reality, and the dialectic (i.e., "reasoning that juxtaposes opposed or contradictory ideas and seeks to resolve conflict"). To illustrate Chinese perspectives, consider the following (Reference 19):

"If we go our own path to develop military theory, weapons, and equipment, we will develop something never seen before in places that no one has ever thought of before; others will be unable to anticipate or resist our 'self-accommodating systems'."

As an illustration of "self-accommodating systems" against the superior foe, three ways are cited for making a cat eat a hot pepper: "stuff it down his throat, put it in cheese and make him swallow it, or grind it up and spread it on his back. The latter method makes the cat lick itself and receive the satisfaction of cleaning up. The cat is oblivious to the end goal. This is strategy."

C. Cyber Deterrence

A vision for "tailored deterrence" was articulated in the 2006 QDR. Consistent with that vision, a recent white paper (Reference 20) identified three aspects of tailoring:

- Tailoring to specific actors and specific situations. This recognizes that tailored deterrence is "context specific and culturally sensitive".
- Tailoring capabilities. One dimension of this factor deals with the associated resource implications.
- Tailoring communications. This relates to the kinds of messages that the US would send in words or actions to deter specific actors, in peacetime and crisis situations.

In order to deal with the various dimensions of tailored deterrence, there are a variety of questions that must be addressed. These questions address, *inter alia,* the social, cultural, and historical aspects of the adversary, including his calculation of risks and gains.

There is a debate within the analytic community as to whether tailored deterrence is a viable concept for the full spectrum of adversaries of the US. That issue represents an important element of the research agenda for the community. However, we believe that the full set of P/DIME capabilities should be considered in developing a course of action to respond to a cyber attack.

D. Cyberstrategy "Rules of Thumb", Principles

In weighing the cyberstrategy insights developed during the course of this study, three key insights emerged. First, the "low end" users (e.g., individuals, hacktivists, terrorists, trans-national criminals) have enhanced their power considerably through recent cyberspace trends. A tailored deterrence strategy will be needed to keep these entities in check.

Second, potential near-peer adversaries are aggressively exploring options to exploit attributes of cyberspace. In the near term, this is being manifested through acts of espionage that have resulted in the exfiltration of massive amounts of sensitive governmental and industrial data. In the longer term, the US must be prepared to deal with unique "cyber strategems" that reflect the unique cultural and military history of key nations (e.g., China, Russia).

To deal with the emerging cyber threat, the US must conduct experiments and exercises that feature a creative and aggressive cyber opposing force. It would be naïve and dangerous to assume that future adversaries will not seek to negate the benefits that the US hopes to achieve through NCW.

V. Theoretical Aspects of Institutional Factors

This section of the paper addresses two institutional factors: governance of cyberspace and selected legal dimensions. It concludes by indentifying key institutional issues and principals.

A. Governance

Table 2 characterizes key governance functions in cyberspace and the organizations

that participate in these functions. It can be seen that the mechanisms for governance of the Internet are *exceedingly* complex. Organizational activities often overlap or fit end-to-end, requiring the expenditure of considerable resources in multiple forums to achieve objectives. Consequently, there is a core set of participants (generally in the private sector) that are involved in several of these key organizations.

Function	ICANN	ISOC*	ITU	OECD	CoE	EU	ISO	IEC	IEEE	W3C	UN
Domain names	•										
International domain names	•		•								
Core Internet functions		•									
Telecommunications standards			•								
World-wide web standards										•	
Product standards			•				•	•	•		
Development			•	•		•					•
Cyber Security**	•	•	•	•	•	•	•	•			

* Internet Society and related organizations (e.g., IETF, IESG, IAB)
** As well as National Governments

Table 2. Governance of Cyberspace

In an effort to evaluate the performance of Internet governance, consider the following criteria: open, democratic, transparent, dynamic, adaptable, accountable, efficient, and effective. When assessed against these criteria, one can conclude that recent Internet governance has performed remarkably well.

However, as we look to future, the USG will be challenged to alter its position on Internet governance. Preliminary views on this subject are being articulated at the ongoing Internet Governance Forums (IGFs). In fact, a recent white paper on the subject (Reference 21) made the following observations:

"Internet Governance is an isolating and abstract term that suggests a nexus with an official government entity. The term also implies a role for the US Congress in Internet decision-making. It is a misnomer because there is no true governance of the Internet; only a series of agreements between a distributed and loosely connected group of organizations and influencers. A more fitting term may be 'Internet Influence,' or for long-term strategy purposes, 'Internet Evolution'."

B. Legal Dimensions

One of the most challenging legal issues confronting the cyber community is as follows: "Is a cyberattack an act of war?" Legalistically, the answer is often presented as one of three possible outcomes: it is not a use of force under UN Article 2(4); it is arguably a use of force or not; it is a use of force under UN Article 2(4).

There are several frameworks that are being considered by the legal community to

address this issue. One of these frameworks, proposed by Mike Schmitt, addresses seven key factors: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility. Once one has assessed each of those factors, one should employ multi-attribute utility theory to weight each of these factors and come to a determination.

Overall, the area of cyber law, is in its infancy. Although there have been preliminary rulings on sharing of music (e.g., Napster), there are major issues on the questions of sovereignty, intellectual capital, and civil liberties. These issues will be major areas for research for the foreseeable future (see Appendix D).

C. Institutional Factors: Key Issues and Principles

Based on the insights developed during the course of this study, four major strawman principles have emerged in the arena of Institutional Factors.

First, given the complexity of the governance mechanisms, one should seek influence over cyberspace vice governance.

Second, the legal community has barely addressed the key issues that must be resolved in the cyber arena. For example, considerable research is needed to assess the following key questions:

- What is an act of (cyber)war?
- What is the appropriate response to an act of (cyber)war?
- What is the appropriate way to treat intellectual property in the digital age?
- How can nations resolve differences in sovereign laws associated with cyber factors?

Third, there is a need for a framework and enhanced dialogue between champions of civil liberties and proponents of enhanced cyber security to establish an adequate balance.

Finally, guidance and procedures are required to address the issue of sharing of cyber information between the USG and industry.

VI. Cyber Modeling, Simulation, and Assessment (MS&A)

Currently, we have a limited set of methods and tools to support policy analysis in the areas of cyberspace, cyberpower, cyberstrategy, and institutional factors (See Figure 8).

In the areas of cyberspace, there are several tools that the community is employing to address computer science and communications issues. Perhaps the best known is the OPNET simulation (Reference 22) that is widely employed to address network architectural issues. From an analytic perspective, techniques such as percolation theory (Reference 23) enable one to evaluate the robustness of a network. Looking to the future, Naval Research Laboratory (NRL) has developed a GIG Testbed to explore the myriad issues associated with linking new systems and networks.

In the area of cyberpower, the community has had some success in employing live, virtual, and constructive (LVC) simulations. For example, in assessments of air-to-air combat, insights have been derived from the live AIMVAL-ACEVAL experiments, virtual experiments in the former McDonnell Air Combat Simulator (MACS), and constructive experiments using tools such as TAC BRAWLER. However, the community still requires better tools to assess the impact of advances in cyberspace on military and informational effectiveness.

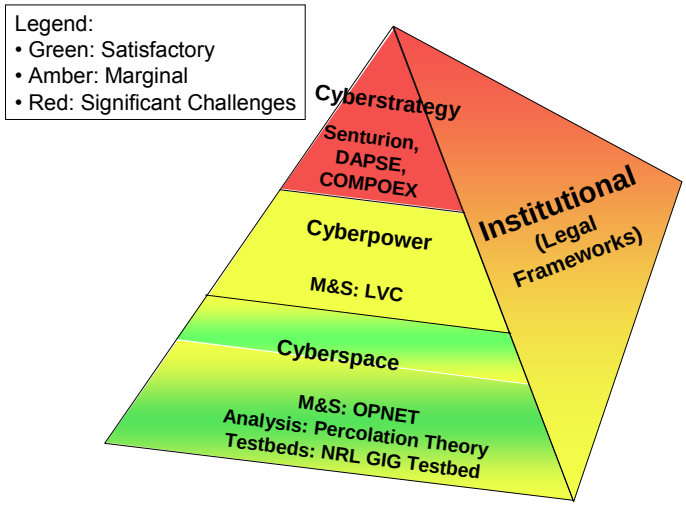


Figure 8. Subjective Assessment of MS&A for Cyber Policy Analyses

In the area of cyberstrategy, a number of promising initiatives are underway. In response to recent tasking by STRATCOM, a new methodology and associated tools are emerging (i.e., Deterrence Analysis & Planning Support Environment (DAPSE) (Reference 24)). However, these results have just been briefed to the Combatant Commands (COCOMs) and they have yet to be applied to major cyberstrategy issues. In addition, promising tools are emerging from academics (e.g., Senturion; GMU's Pythia) and DARPA (e.g., Conflict Modeling, Planning & Outcomes Experimentation (COMPOEX)). However, these are still in early stages of development and application.

Finally, as noted above, there are only primitive tools available to address issues of governance, legal issues, and civil liberties. Some tools are being developed to explore the cascading effects among critical infrastructures (e.g., National Infrastructure Simulation and Analysis Center (NISAC) system dynamics models); however, they have not yet undergone rigorous validation.

VII. Connections

At the beginning of this paper, it was noted that one of the reasons for a theory was the need to **connect** diverse elements of a body of knowledge. In general, the community is focusing on the issue of connecting the knowledge within a layer of the pyramid. Even though this is challenging, it generally involves communicating among individuals with a common background and lexicon.

It is far more difficult to have individuals connect **across** the different layers of the pyramid. This requires individuals from different disciplines to work effectively together. In order to do so, it requires a holistic perspective on the Measures of Merit (MoMs) for cyber issues.

Table 3 suggests a potential decomposition of the MoMs associated with the cyber problem. It identifies four linked sets of measures: Measures of Performance (MoPs), Measures of Functional Performance (MoFPs), Measures of Effectiveness (MoEs), and

Measures of Entity Empowerment (MoEEs). Since this field of endeavor is still in its infancy, the material is meant to be illustrative and not exhaustive. Additional comments on MoMs are provided in Appendix C.

Measures	Representative Measures
Entity Empowerment	• **P**olitical reforms (e.g., participation in democratic elections) • **M**ilitary efforts to enhance security (e.g., reduction in number, severity of insurgent, terrorist attacks) • **E**conomic reforms (e.g., reconstruction projects completed effectively) • **S**ocial reforms (e.g., reconciliation of warring parties) • **I**nformation (e.g., gaining trust of host nation population) • **I**nfrastructure (e.g., improvement in delivery of electric power, clean water)
Effectiveness (against targeted groups)	• Media: Number of positive/negative stories published/aired • Clerics: Tone of mosque sermons • Military: Loss Exchange Ratios
Functional Performance	• Time to create, validate, disseminate influence messages • Number of meetings held with surrogate groups
Performance	• System performance (e.g., latency, bandwidth, reliability) • Resistance to adversary attack (e.g., ability to withstand a Denial of Service attack)

Table 3. Selected Measures of Merit

VIII. Summary

Consistent with the macro-framework that has been adopted to characterize the cyber problem, the evolving theory of cyberpower has given rise to key insights into the nature of the problem in the areas of cyberspace, cyberpower, cyberstrategy, and institutional factors.

A. Cyberspace

Cyberspace is a man-made environment that is experiencing exponential growth in key MoPs. There is an extraordinary diffusion of knowledge among all the stakeholders of cyberspace, including malevolent users. As a consequence of this diffusion of knowledge, cyberspace is being degraded by "noise" (e.g., proliferation of spam) and a broad variety of cyber attacks. The most troubling of these attacks includes Denial of Service, exfiltration of data, and the potential for corruption of data. In each instance, recent experience has demonstrated that these attacks are relatively easy to implement (e.g., technically, financially) and extremely difficult to attribute.

These vulnerabilities arise from the basic architecture that has evolved from the original ARPAnet. A new cyberspace architecture may be required to halt the perceived erosion of security. However, there will be substantial difficulties in transitioning from the current architecture to one that is more robust against adversary action.

B. Cyberpower

As cyberspace evolves, it has the potential to enhance each of the levers of national power. This paper has focused on two of these levers: military and information.

In the area of military power, it was observed that studies are underway to characterize the extent to which enhancements in cyberspace can enhance key MoEs.

These studies tend to be unambiguous in the area of air-to-air combat where experiments suggest that enhanced digital communications can enhance loss-exchange ratios by a factor of approximately 2.5. Although studies of other military operations have also been undertaken, the results are generally confounded by other factors (e.g., mobility, protection).

To complement these experiments, an assessment of theories of environmental warfare was undertaken that critically reassessed the theories of land, sea, air, and space theory. Based on that assessment, it was concluded that a theory of cyberpower should focus on four key factors: technological advances, speed and scope of operations, control of key features, and national mobilization.

From the perspective of "information", the paper has addressed influence operations from a strategic and tactical perspective. Based on prior experiences and an adaptation of earlier analytical frameworks, an approach was developed for linking operational objectives and processes to DOTMLPF requirements. These assessments suggest that developments in cyberspace can substantially affect future efforts to enhance influence operations (e.g., implement precision guided *messages*).

C. Cyberstrategy

The evolving theory of cyber has identified a range of entities that will be empowered by enhancements in cyberspace. These include: terrorist groups, who are employing cyberspace to, *inter alia*, recruit, raise money, propagandize, educate and train, plan operations, command and control operations; hacktivists, who are employing cyberspace to conduct "cyber riots" (e.g., Estonia) and implement exploits in cyberspace; transnational criminals, who pursue a variety of techniques (e.g., phishing, denial of service attacks) to raise substantial funds (reputed to be more than the money derived from drug trafficking); and nation states, the most advanced of whom are employing cyberspace to enhance all dimensions of PMESII activities;

However, changes in cyberspace have given rise to unintended consequences. Many of the entities at the "low end" of the entity spectrum (e.g., terrorists, hacktivists, transnational criminals) are making life more dangerous for information-enabled societies. In particular, these entities tend to be much more adaptable than nation states, causing the latter to respond, belatedly, to the initiatives of the former. In addition, research about selected near-peers (e.g., China, Russia) suggests that they have new perspectives on cyberstrategy that will present information-enabled societies with new challenges in cyberspace.

D. Institutional Factors

From an institutional perspective, issues are emerging that will affect all aspect of cyber theory. This paper has highlighted the challenges that exist in cyber governance (or influence) and cyber legal issues.

From a theoretical perspective, one of the major challenges emerges from the difficulty in characterizing and responding to an attack in cyberspace. As demonstrated by recent events in Estonia, it is extremely difficult to attribute an attack to an adversary that chooses to act anonymously. In light of that ambiguity, it is difficult to formulate a coherent response to such an attack. For example, it is still unclear how an alliance, such as NATO, might respond in the future to a cyber attack against one or more of its members. It is anticipated that these issues will be addressed in subsequent analyses.

Appendix A. Timeline of Key Cyber Events

This appendix summarizes several of the key events associated with the evolution of cyberspace, cyberpower, cyberstrategy, and institutional factors. These observations have affected the formulation of the preliminary theory of cyberpower.

A.1 Evolution of Cyberspace

Figure A.1 provides a timeline of key recent events that have shaped cyberspace. It is notable that this timeline is scarcely 40 years old. Among the key events of interest are the creation of the Internet (and the associated development of the Transmission Control Protocol/Internet Protocol (TCP/IP)) and the evolution of the Domain Name Service (DNS). A major enabler was the proliferation of inexpensive personal computers with

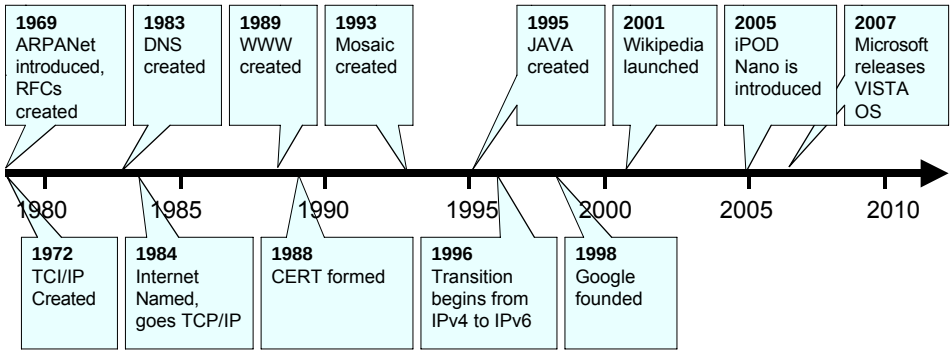


Figure A.1. Evolution of Cyberspace

operating systems (e.g., Microsoft Windows) that made it relatively simple for any user to employ the technology. Other seminal events include the creation of the World Wide Web and the Mosaic browser that made the information easily accessible to individual users. During this period, the transition from IPv4 to IPv6 also got underway, with the new protocol marking a great improvement in address space and providing greatly enhanced flexibility in assigning addresses.

More recently, a milestone was reached in 1997, when e-mail use surpassed that of regular mail for the first time. Google was founded in 1998 and it has become the world leader in popular search engines. By virtue of its advertising revenue, it has developed a viable business model. By 1999, WIFI technology began to proliferate, enabling wireless Internet connection, thus achieving significantly greater interconnectedness then ever before.

Other important developments involved the launch of Pay-Pal in 2000 and Wikipedia

in 2001. Their open source software is widely used by key government entities (e.g., Intellipedia; Joint Data Systems of the Office of the Secretary of Defense). Their implications on empowerment of the individual are discussed below.

In 2001, Apple began to sell the ubiquitous iPod. As discussed below, that device is able to provide high capacity in an extremely small package due to the discovery of giant magnetoresistance. Another idea with evolutionary effect is the Semantic Web, which serves as an extension to the World Wide Web and allows for better information sharing and integration.

Finally, in 2007, Microsoft released VISTA, a new Operating System (OS). The oft-delayed product was revised to deal with the many security problems that afflict cyberspace.

A.2 Evolution of Cyberpower

The timeline in Figure A.2 identifies several key events that have shaped the military's perspectives on the use of cyberspace. The timeline begins in 1983 when MILNET split off from ARPANET (subsequently becoming the Defense Data Network). Subsequently, the intellectual underpinnings of military cyberpower were refined by the publication of Joint Vision 2010 (Reference 25). That was complemented by the Advanced Battlespace Information System (ABIS) which was co-sponsored by Vice Admiral Arthur Cebrowski, Director, J6, Joint Staff, and Dr. Anita Jones, DDR&E, to orchestrate evolving net concepts of operations and science and technology (S&T) investments (Reference 26). Subsequently, Vice Admiral Cebrowski and John Gartska wrote a seminal paper in the Proceedings of the Naval Institute that introduced the concept of Net Centric Warfare (NCW) (Reference 27). Building on that base, OSD introduced the concept of the GIG and the individual Services formulated their visions of subordinate networks (e.g., the USN ForceNet, the USA LandWarNet, the USAF C2 Constellation). In addition, selected NATO and Partnership for Peace nations developed tailored strategies to implement variants of Net Enabled Capabilities. More recently, the USAF has modified their mission space to include operations in cyberspace and reorganized to create an Air Cyber Command (Reference 28).

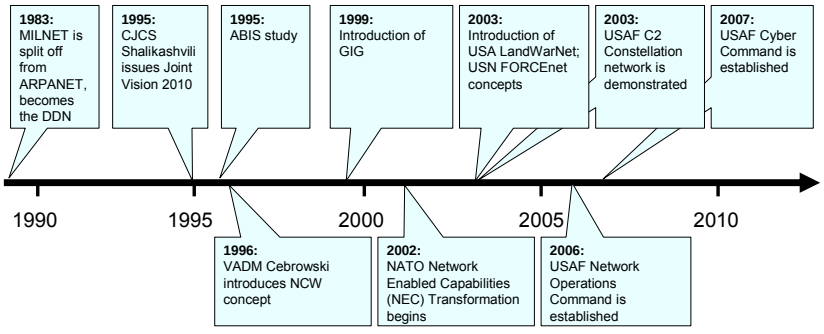


Figure A.2. Evolution of Cyberpower: Military Perspective

Although the current NDU effort has not specifically addressed the economic and diplomatic levers of power, these issues are being actively discussed elsewhere. For example, in Thomas Friedman's book, "The World is Flat", he identifies ten key steps on the road to increased economic globalization (Reference 29). As seen in Figure A.3, these steps have their roots deep within the use of information technology (e.g., the age of the personal computer, advent of the Internet, revolution in Internet search engine capabilities). The extent and impact of globalization are being actively debated in the academic community.

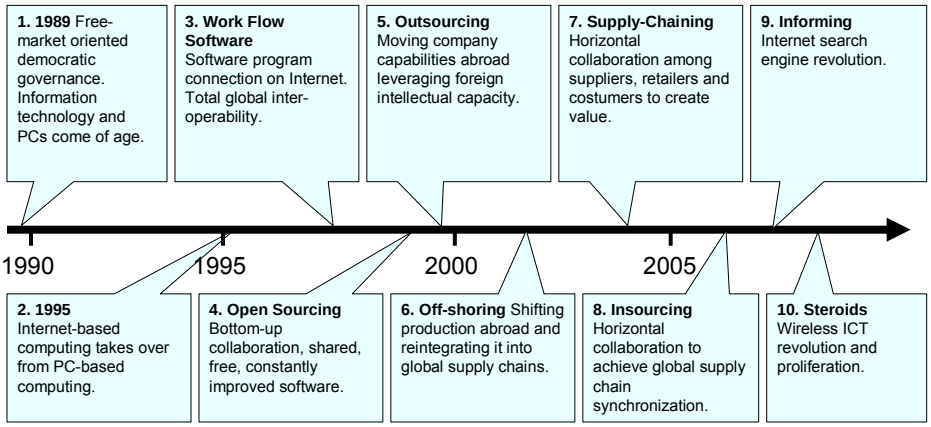


Figure A.3. Evolution of Cyberpower: Economic Perspective

Similarly, the Diplomatic community is beginning to assess the impact of cyberspace on its operations. It has been noted that the global availability of information has affected the roles of embassies. Where once the embassy was the primary source of indigenous information, the capital city frequently has access to information that is not easily available to the embassy. Furthermore, the Department of State has begun to explore "blog" diplomacy to provide "digital outreach" (Reference 30).

A.3 Evolution of Cyberstrategy

The cyberstrategy timeline in Figure A.4 emphasizes selected attacks and responses in cyberspace. At the onset of the timeline, the key elements of malware included worms (1979) and viruses (1983). An early example of an attack on sensitive but unclassified USG systems occurred in 1998 with the advent of Solar Sunrise. Although this was ultimately attributed to two California teenagers (linked to a subject matter expert in Israel), it dramatized the vulnerability of selected USG data bases to intrusion. Subsequently, events such as Moonlight Maze (beginning in 1999 and attributed to sources in Russia) and Titan Rain (beginning in 2003 and attributed to sources in China) suggested the vulnerability of USG and defense industrial base data sources to cyber

espionage. In the case of Titan Rain, it has been estimated that Chinese sources have exfiltrated on the order of 10 terabits of data.

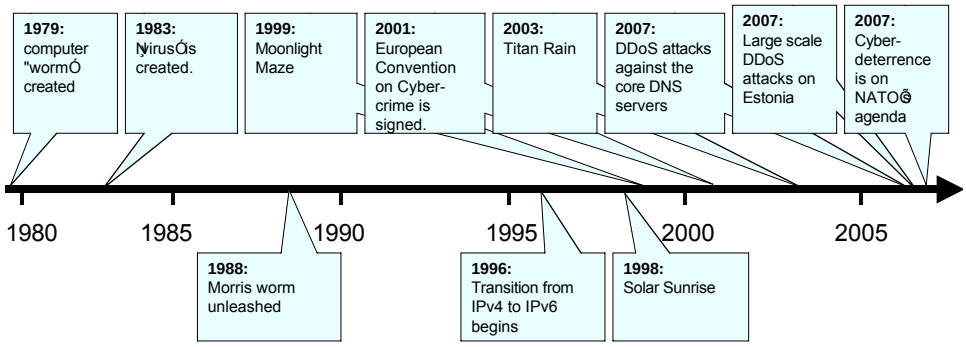


Figure A.4. Evolution of Cyberstrategy: Selected Attacks and Responses

More recently, attacks have featured distributed denial of service (DDOS), drawing on herds of penetrated zombies or bots. As examples, in February 2007 there was a (generally unsuccessful) attack on the core DNS servers (Reference 31) and a reasonably successful "cyber riot" against key sectors of Estonia (e.g., government, financial sector, media outlets) (Reference 32). In many of these events, it has proven exceedingly difficult to attribute the source of the attack.

The attack against Estonia has prompted NATO to re-evaluate its position on cyber defense. For example, Estonia is in the process of establishing a Computer Defense Center of Excellence and NATO is placing cyber deterrence on its agenda for forthcoming senior meetings. With respect to the latter, there is on-going discussion about the implications of a cyber-attack against a NATO ally (e.g., Is an "attack against one, an attack against all"? Does it have ramifications for Articles 4 and 5?).

A.4 Evolution of Institutional Factors

Figure A.5 provides a timeline of key institutional events. As context, several of the early events (e.g., demonstration of the ARPANet, introduction of TCP/IP into the Internet, creation of the DNS) have been discussed above.

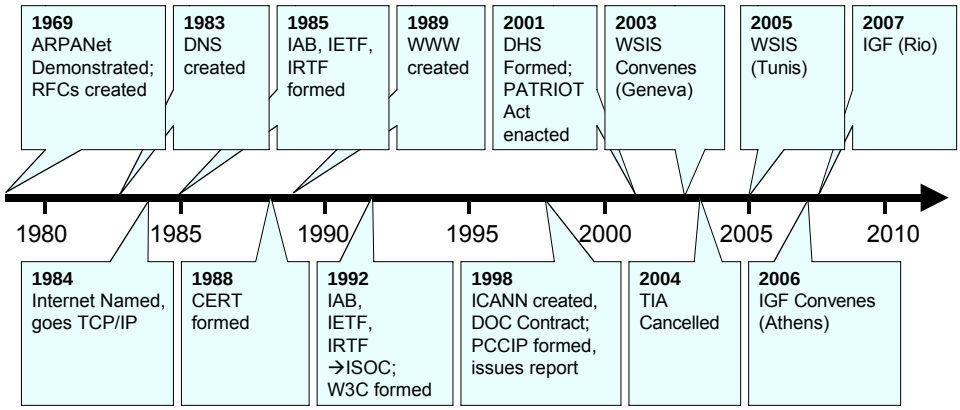


Figure A.5. Timeline of Key Institutional Events

In the 1980-1990s, several organizations were created to provide governance for the Internet (e.g., Internet Engineering Task Force (IETF), Internet Research Task Force (IRTF)). As can be seen, in 1992, they morphed into the Internet Society (ISOC) and the World Wide Web Consortium was formed. Subsequently, the Internet Corporation for Assigned Names and Numbers (ICANN) was created in 1998.

In 1998, the President's Commission on Critical Infrastructure Protection (PCCIP) was formed under the leadership of General Tom Marsh. That effort focused public attention on the issues associated with CIP.

Institutionally, the events of September 11, 2001, gave rise to significant organizational and legal activities. These included the creation of the Department of Homeland Security and the passage of the Patriot Act. One unintended consequence was the formation and cancellation of the Total Information Awareness (TIA) program at DARPA, due in part to concerns voiced by civil liberties advocates.

In recent years, the future governance of the Internet is being affected by two meetings of the World Summit on the Information Society (WSIS) (in Geneva and Tunis). These have been followed by two Internet Governance Forum (IGF) meetings, in Athens and Rio de Janeiro, respectively.

Appendix B. Recommendations of the Special Report on Internet-Facilitated Radicalization

The Special Report on Internet-Facilitated Radicalization formulated five recommendations to address the cyber threat posed by terrorists (Reference 17).

First, they recommended that we craft a compelling counter-narrative for worldwide delivery, in multimedia, at and by the grassroots level. Subordinate aspects of this recommendation include: challenging extremist doctrine; offering a compelling narrative that pulls potential extremists back from the brink; using graphic visuals to magnify the impact of language; building on core values common to all; delivering the message through authentic sources; and amplifying and augmenting non-extremist voices emanating from the grassroots.

Second, they recommended that we foster intra- and cross-cultural dialogue and understanding to strengthen the ties that bind together communities at the local, national, and international levels. This includes: addressing the perceptions and realities of American Muslim alienation and marginalization; enhancing civic engagement; increasing people-to-people exchanges; and dealing appropriately with the media.

Third, they recommended that we recognize and address the need for additional behavioral science research into the process of radicalization both online and offline. This includes: deepening our understanding of the process of radicalization to further inform counter-strategy; and applying social networking theory.

Fourth, they recommended that we deny or disrupt extremist access to, and extremist efforts through, the Internet via legal and technical means, and covert action, where appropriate. This includes: invoking the full force of the law where it makes most sense to do so; and undermining the trust that binds enemy networks. They also emphasized the need to fully appreciate and skillfully exploit the convergence of human intelligence and cyberspace.

Finally, they recommended that we remedy and resource capability gaps in government. To implement that recommendation, they cited four subordinate actions: address deficits in linguistic and cultural knowledge, skills, and abilities; choose words carefully to reclaim the high ground; remedy the lack of a strategic communications plan; and expand community policing programs.

Appendix C. Measures of Merit

Figure C.1 suggests a potential decomposition of the MoMs associated with the cyber problem into MoPs, MOFPs, MoEs, and MoEEs.

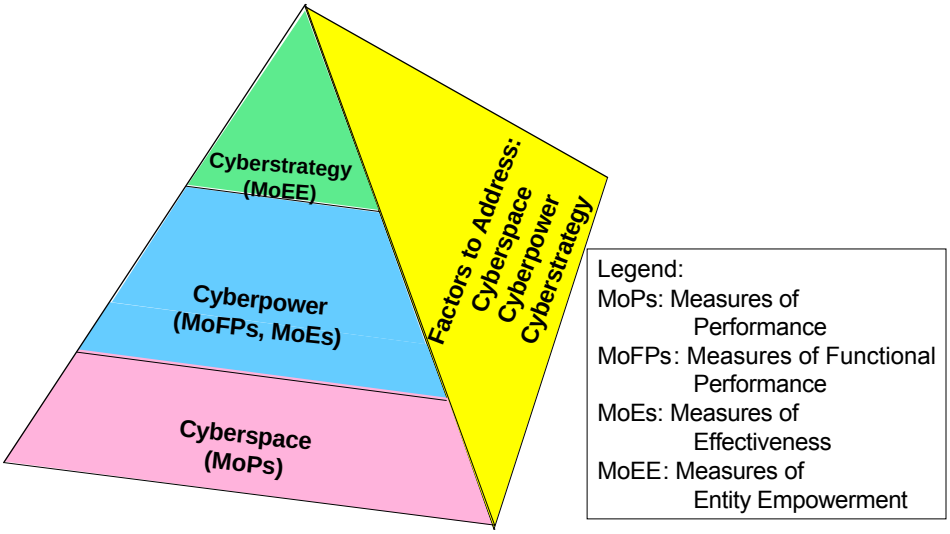


Figure C.1. Measures of Merit

MoPs are needed to characterize the key computer science and electrical engineering dimensions of the problem. A key measure is the amount of bandwidth that is available to representative users of cyberspace. As the bandwidth increases to the megahertz/sec range, the user is able to access advanced features such as imagery and video products. A second key measure is connectivity. For circumstances in which the cyber-infrastructure is fixed, a useful measure is the percent of people in a country that have access to the Internet. However, in many military operations, the cyber-infrastructure and the users are mobile. Under those circumstances, a more useful measure is the performance of Mobile, Ad hoc NETwork (MANET) users (e.g., their ability to stay connected). Third, one can introduce measures of the "noise" that characterizes the cyber-infrastructure. For example, the extent to which the quality of the Internet is degraded can be characterized by the unwanted e-mail that it carries ("spam"), which can subsume a substantial subset of the network's capacity. As an example, it has been estimated that in recent months approximately 90% of the traffic on the Internet is spam (Reference 43). In addition, the integrity of the information is further compromised by "phishing" exploits in which criminal elements seek to employ the Internet to perpetrate economic scams. Finally, MoPs can be introduced to characterize resistance to adversary actions, including denial of service attacks, propagation of viruses or worms, and illicitly intruding into a system.

It is useful to introduce MoFPs that characterize how successfully selected entities are able to perform key functions, taking advantage of cyberspace. In the case of the US military, the concept of net-centricity is to employ advances in cyberspace to perform

essential functions. These include the ability to enhance the performance of increasing levels of information fusion (e.g., at level 1, the ability to generate a timely, complete, accurate picture of Blue forces). Similarly, a basic tenet of net-centricity is to propagate commander's intent so that the participants in the operation can synchronize and self-synchronize their actions.

MoEs are needed to characterize how effective entities can be in their key missions, taking advantage of cyberspace. In the context of Major Combat Operations, MoEs are needed to characterize the ability to exploit cyberspace in multiple dimensions. At one extreme, enhancements in cyberspace have the potential to reduce the time to conduct a campaign and the casualties associated with the campaign. At the other extreme, enhancements in cyberspace may substantially enhance Blue loss exchange ratios and the amount of ground gained and controlled.

From the perspective of cyberstrategy, there is interest is characterizing the extent to which enhancements in cyberspace can empower key entities. In the case of nation states, potential MoEEs might include the ability to leverage cyberspace to influence a population (e.g., "win hearts and minds"), shape a nation at strategic crossroads, and deter, persuade, and coerce an adversary.

Appendix D. Opportunities for Cyber Research

As an application of the emerging theory of cyberpower, this appendix explores major cyber research activities that should be pursued to address key challenges. Table C-1 summarizes the major areas where research should be pursued. The remainder of this appendix discusses each of these proposed initiatives.

Area	Research Areas
Cyberspace	• Perform technology projections to identify key breakthroughs • Develop techniques to protect essential data from exfiltration, corruption • Formulate an objective network architecture that is more secure, and identify options to transition to it
Cyberpower	• Extend analyses to other levers of power (e.g., diplomatic, economic) • Perform risk assessments to address cyber-dependence • Quantify the Blue-Red information duel
Cyberstrategy	• Conduct research on "tailored deterrence" • Explore options to address cyber espionage
Institutional Factors	• Perform research on cyber influence; legal frameworks; balance between security and civil liberties
Cyber Assessment	• Develop analytical methods, tools, data, and intellectual capital to assess cyber issues

Table D-1. Areas Where Additional Theoretical Research Are Required

D-1. Cyberspace

In the area of cyberspace, improved technology projections are needed to identify key breakthroughs that may substantially affect MoPs for cyberspace (e.g., breakthroughs comparable to the discovery of giant-magnetorestance). Second, it is inevitable that malevolent actors (e.g., insiders, adaptive adversaries) will gain access to the USG and defense industrial base cyberspace. This suggests that research is needed to protect the essential data in cyberspace from exfiltration or corruption. Finally, additional research is needed to formulate an objective architecture for cyberspace that is inherently more secure than the existing architecture. Consistent with that effort, there is a need to address the challenging issue of transitioning from the existing to the objective architecture.

D-2. Cyberpower

Due to resource constraints, this preliminary assessment of cyber theory has not adequately addressed all the levers of power (e.g., political, diplomatic, economic). As an initial step, assessments should be completed for these other levers of power. Second, existing assessments of the military lever of power have focused almost exclusively on the potential benefits that can accrue by creatively employing cyberspace. It is equally important to perform risk assessments to understand the potential downside of relying extensively on cyberspace. This includes conducting experiments and developing the methodology, tools, data, and intellectual capital required to perform military risk assessments. Similarly, it is important to conduct research into the potential benefits and

risks associated with leveraging cyberspace developments for non-US military capability (e.g., NATO allies that are pursuing Network Enabled Capabilities (NEC)). Finally, in the area of information, additional research is needed to quantify the information duels that are likely to occur between Blue and Red actors.

D-3. Cyberstrategy

To deal with the challenges posed by the full array of entities empowered by enhancements in cyberspace, it is vital that the information-enabled societies conduct research on "tailored deterrence". This concept suggests that key alliances, such as NATO, must develop a holistic philosophy that understands each of the potential adversaries (e.g., its goals, culture, risk calculus), develops and plans for capabilities to deter these adversaries, and develops a strategy to communicate these concepts to the potential adversaries.

D-4. Institutional Factors

Theoretical research is needed to address key gaps in institutional knowledge in the areas of governance, legal issues, sharing of information, Internet regulation, and civil liberties.

First, in the area of governance, the USG must reassess the role of ICANN in the governance of the Internet. It is clear that, in the future, the USG must be more adroit in the area of "cyber influence" vice governance. This will require a thorough re-examination of all the institutional bodies that affect cyber governance and the development of a USG strategy to interact with them.

Second, "cyber legal" issues are in their infancy. The current situation is non-homogeneous with inconsistent laws in various sovereign nations (e.g., German hate-crime laws; limited signatories to the European Convention of Cybercrime). In particular, there is a need to clarify the issue of espionage in cyberspace (e.g., What is it? What rights of response are left to the victims?). In addition, there is a need to adopt a consistent model that can be applied to determine whether a cyber attack is an act of war.

Third, there is continued controversy about the sharing of information between the USG and industry. Research is needed to determine what information should be shared, under what circumstances.

Fourth, it has been observed that regulatory agencies, such as the Federal Communications Commission, have the authority to regulate ISPs to redress selected cyber security issues. However, to date, regulatory agencies have been reluctant to address these issues.

Fifth, the recent debate about the Foreign Intelligence Surveillance Act (FISA) court has mobilized the civil liberties community to raise the specter of "Big Brother". As a consequence of the actions of civil liberties organizations, key USG programs have been terminated or modified (e.g., TIA, Multi-state Anti-Terrorism Information Exchange (MATRIX)). Research is needed to clarify the appropriate balance among actions to deal with adversaries (e.g., terrorists) while still protecting civil liberties.

D-5. Cyber Assessment

As discussed in the main body of the paper, our ability to perform cyber assessments is extremely uneven. As a consequence, research efforts are required to develop analytical methods, tools, data, and intellectual capital to address key cyber issues in the areas of cyberpower, cyberstrategy, and infrastructure issues.

Appendix E. Abbreviations and Acronyms

Abbreviation/Acronym	Definition
ABIS	Advanced Battlespace Information System
C2	Command and control
CEA	Council of Economic Advisers
COMPOEX	Conflict Modeling, Planning & Outcomes Experimentation
CNA	Computer Network Attack
CNO	Computer Network Operations
CTNSP	Center for Technology and National Security Policy
DAPSE	Deterrence Analysis & Planning Support Environment
DARPA	Defense Advanced Research Projects Agency
DIME	Diplomatic, Information, Military, Economic
DNS	Domain Name System
DoD	Department of Defense
DoS	Denial of Service
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, Facilities
GIG	Global Information Grid
HBSC	Human, Behavior, Social, and Cultural
IAB	Internet Architecture Board
ICANN	Internet Corporation for Assigned Names and Numbers
IED	Improvised Explosive Device
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
INSS	Institute for National Strategic Studies
IP	Internet Protocol
IRTF	Internet Research Task Force
ISOC	Internet Society
JMEM	Joint Munitions Effectiveness Manual
JTRS	Joint Tactical Radios System
JWICS	Joint Worldwide Intelligence Communications System
MACS	McDonnell Air Combat Simulator
MANET	Mobile Ad Hoc Network
MoE	Measure of Effectiveness
MoEE	Measure of Entity Empowerment
MoFP	Measure of Functional Performance
MoM	Measure of Merit
MoP	Measure of Performance
NATO	North Atlantic Treaty Organization
NCO	Net Centric Operations
NCW	Net Centric Warfare
NDU	National Defense University
NEC	Net Enabled Capability

NMS-CO	National Military Strategy for Cyber Operations
NRL	Naval Research Laboratory
OLPC	One Laptop Per Child
OODA	Observe-Orient- Decide-Act
OS	Operating System
OSD	Office of the Secretary of Defense
P/DIME	Political/ Diplomatic, Information, Military, Economic
PMESII	Political, Military, Economic, Social, Information, Infrastructure
QDR	Quadrennial Defense Review
R&D	Research & Development
SME	Subject Matter Expert
SOA	Service Oriented Architecture
SSG	Strategic Studies Group
SSTR	Stability, Security, Transition, Reconstruction
STRATCOM	Strategic Command
TIA	Total Information Awareness
TCP	Transmission Control Protocol
ToR	Terms of Reference
UDP	User Datagram Protocol
USG	United States Government
VOIP	Voice over Internet Protocol
WIMAX	Worldwide Interoperability for Microwave Access
WSIS	World Summit on the Information Society

Appendix F. References

1. 2006 Quadrennial Defense Review (QDR), Office of the Secretary of Defense, 6 February 2006.
2. Charles D. Lutes, "INSS Project Summary: Towards a Theory of Spacepower", August 28, 2007.
3. Terms of Reference for study of "A Theory of Cyberpower", March 2006.
4. Dr. Harold R. Winton, Air War College, Maxwell AFB, "An Imperfect Jewel: Military Theory and the Military Profession", presented at INSS workshop on theory of warfare, NDU, Washington, DC, September 2006.
5. Strategic Studies Group XXVI, "Convergence of SeaPower and CyberPower", July 24, 2007.
6. William Gibson, "Neuromancer", Ace Science Fiction, 1984.
7. "National Military Strategy for Cyberspace Operations (NMS-CO)", Joint Staff, December 2006.
8. Jeremy M. Kaplan, "A New Conceptual Framework for Net-Centric, Enterprise Wide, System-of-Systems Engineering," CTNSP/NDU, Number 29, July 2006.
9. Philip E. Ross, "5 Commandments", IEEE Spectrum, Vol. 40, Issue 12, December 2003.
10. Audi Lagorce, "Clearwire, Sprint Nextel Scrap WiMax Network Agreement", Market Watch, November 9, 2007.
11. David T. Signori and Stuart H. Starr, "The Mission Oriented Approach to NATO C2 Planning", Signal Magazine, PP 119 – 127, September 1987.
12. Colonel Ralph Baker, "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations", Military Review, May-June 2006.
13. George Gilder, "Metcalfe's Law and Legacy", Forbes ASAP, 13 September 1993.
14. Bob Briscoe, Andrew Odlyzko, Benjamin Tilly, "Metcalfe's Law is Wrong", IEEE Spectrum, July 2006.
15. Daniel Gonzales, et al, "Network-Centric Operations Case Study: Air-to-Air Combat With and Without Link 16", RAND, National Defense Research Institute, 2005.
16. Gabriel Weimann, "Terror on the Internet: The New Arena, The New Challenge", US Institute for Peace, Washington, DC, 2006.
17. Homeland Security Policy Institute, "NETworked Radicalization: A Counter-Strategy", GWU, Washington, DC, May 2007.
18. Joseph S. Nye, Jr., "Understanding International Conflicts: An Introduction to Theory and History", New York: Pearson-Longman, 2005.
19. Tim Thomas, "Chinese Perspectives on Cyberstrategy", presentation at CTNSP/NDU workshop, Washington, DC, November 8, 2006.
20. M. Elaine Bunn, "Can Deterrence Be Tailored?", Strategic Forum, Institute for National Strategic Studies, National Defense University, No. 225, January 2007.
21. OASD(NII)/DOD CIO Globalization Task Force, "Development of an Internet Influence/Evolution Strategy for the Department of Defense", October 19, 2007.
22. Emad Aboelela, "Network Simulation Experiments Manual", Morgan Kaufmann, publisher; 3rd edition, June 2003.

23. Ira Kohlberg, “Percolation Theory of Coupled Infrastructures”, 2007 Homeland Security Symposium, “Cascading Infrastructure Failures: Avoidance and Response”, National Academies of Sciences, Washington, DC, May 2007.
24. Strategic Multi-Layer Analysis Team (Nancy Chesser, Editor), “Deterrence in the 21st Century: An Effects-Based Approach in An Interconnected World, Volume I”, sponsored by USSTRATCOM Global Innovation and Strategy Center, 1 October 2007.
25. GEN John M. Shalikashvilli, CJCS, “Joint Vision 2010”, July 1996.
26. Arthur Cebrowski and Anita Jones, “Advanced Battlespace Information System: Volume I”, 1996
27. Arthur Cebrowski and John Gartska, “Network Centric Warfare: Its Origin and Future”, US Naval Institute Proceedings, January 1998.
28. Josh Rogin, “Air Force to Create Cyber Command”, FCW.COM, November 13, 2006.
29. Thomas L. Friedman, “The World is Flat: A Brief History of the Twenty-First Century”, Farrar, Strauss and Giroux, 2005.
30. Walter Pincus “State Department Tries Blog Diplomacy”, Washington Post, November 19, 2007, page A15.
31. ICANN Factsheet, “Root server Attack on 6 February, 2007”, 1 March 2007.
32. Joshua Davis, “Hackers Take Down the Most Wired Country in Europe”, Wired Magazine, Issue 15.09, August 22, 2007.

Towards a (Preliminary) Theory of Cyberpower

Frank Kramer, Stuart Starr, Larry Wentz
Center for Technology and National Security Policy (CTNSP)
National Defense University (NDU)

June 17, 2008

Objective, Approach

- Objective
  - "… there is a compelling need for a **comprehensive, robust and articulate cyber power theory** that describes, explains and predicts how our nation should best use cyber power in support of US national and security interests" (2006 QDR)
- Approach
  - Multiple workshops were convened to develop the chapters of a book
  - This was complemented by three efforts; we
    - Drew insights from observations of events, experiments, and trends
    - Built on prior national security methods, frameworks, theories, tools, data, and studies
    - Formulated and hypothesized new methods, frameworks, theories, and tools to deal with unexplained trends, issues

Why a Theory?

- A Theory of Cyberpower will serve to
  - Define
  - Categorize
  - Explain
  - Connect
  - Anticipate
- However, as a caveat, any preliminary theory of cyberpower will
  - **Not** be complete
  - Be, at least, somewhat **wrong**

Cyber Theory Challenges

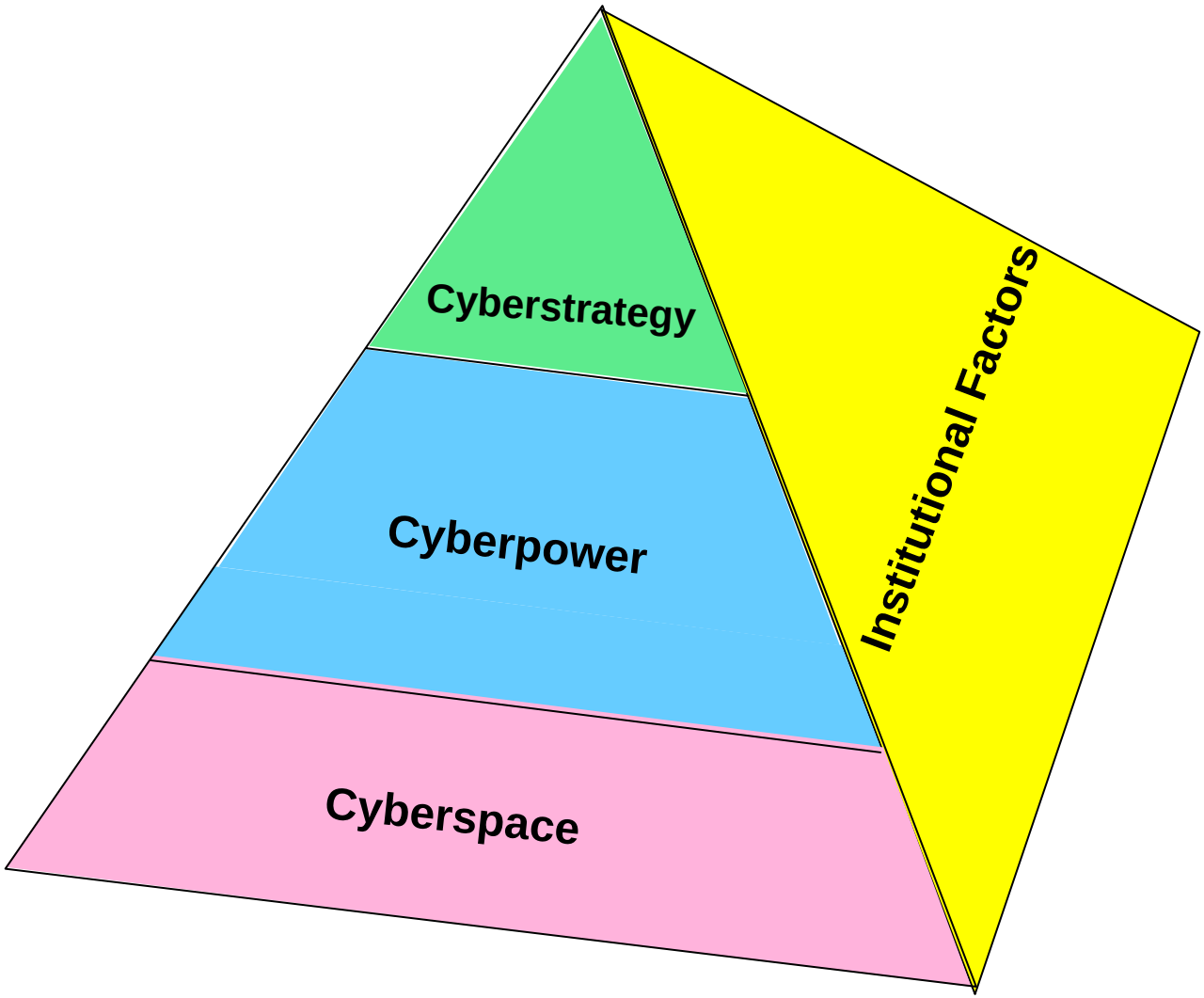
- Timeframe: several decades
- Discipline: subsumes multiple disciplines (e.g., hard and soft sciences, professions), most of whom can not communicate effectively
- Definitions: most basic terms are still contentious
- Categorize: no agreed upon taxonomy
- Explain, anticipate
  - The field is changing exponentially (in the midst of “a tipping point”)
  - Little or no agreement on key frameworks
  - Ability to explain is limited, particularly for social science aspects
  - Reliable prediction is infeasible
- Connect: A holistic perspective has not yet been created

A Theory Will Serve to *Define*…

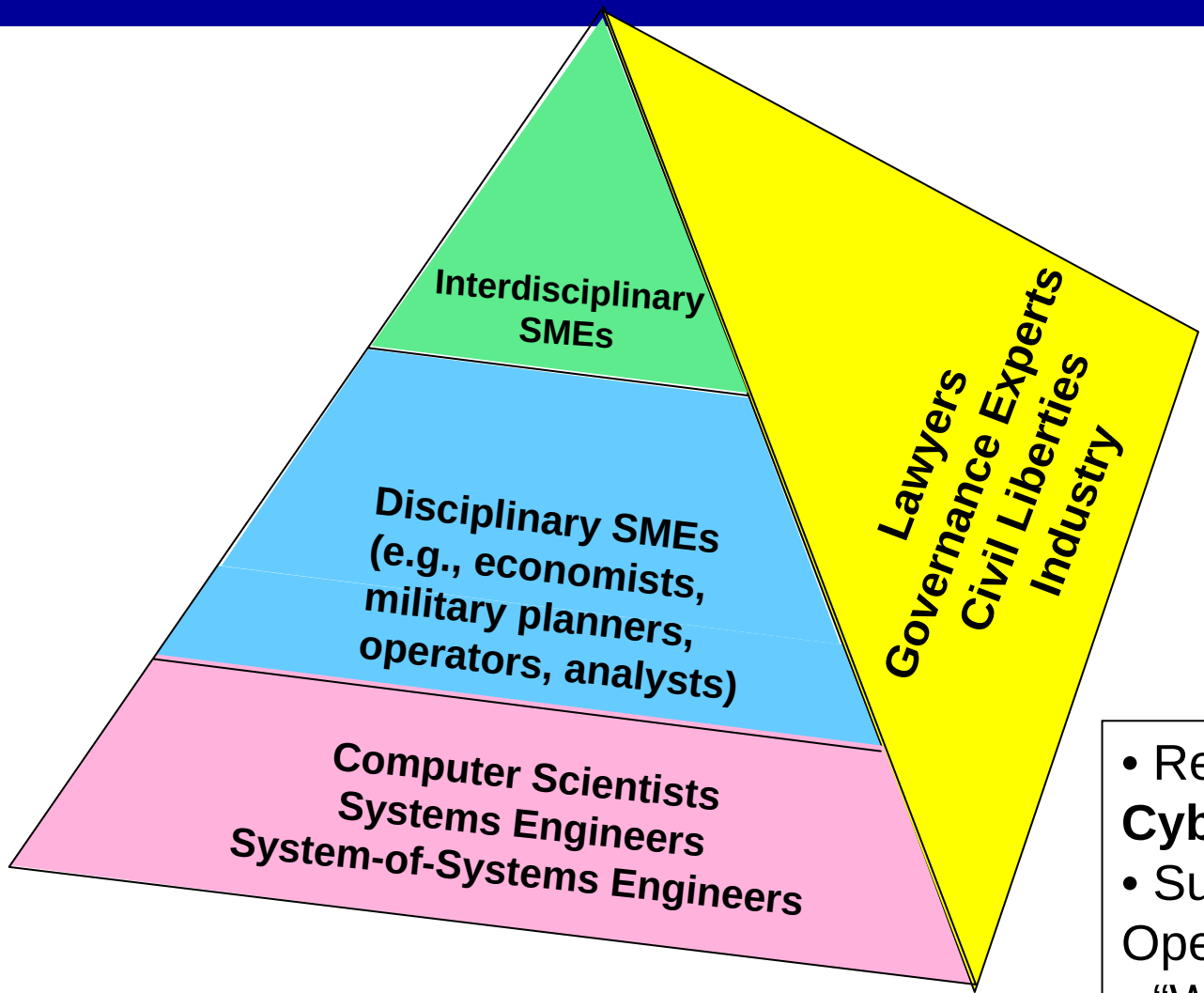
- Cyberspace is an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and internetted information systems and their associated infrastructures."
- **Cyberpower** is the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power
- **Cyberstrategy** is the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power

Source: Dan Kuehl, IRMC, NDU

A Theory Will Serve to *Categorize* Areas



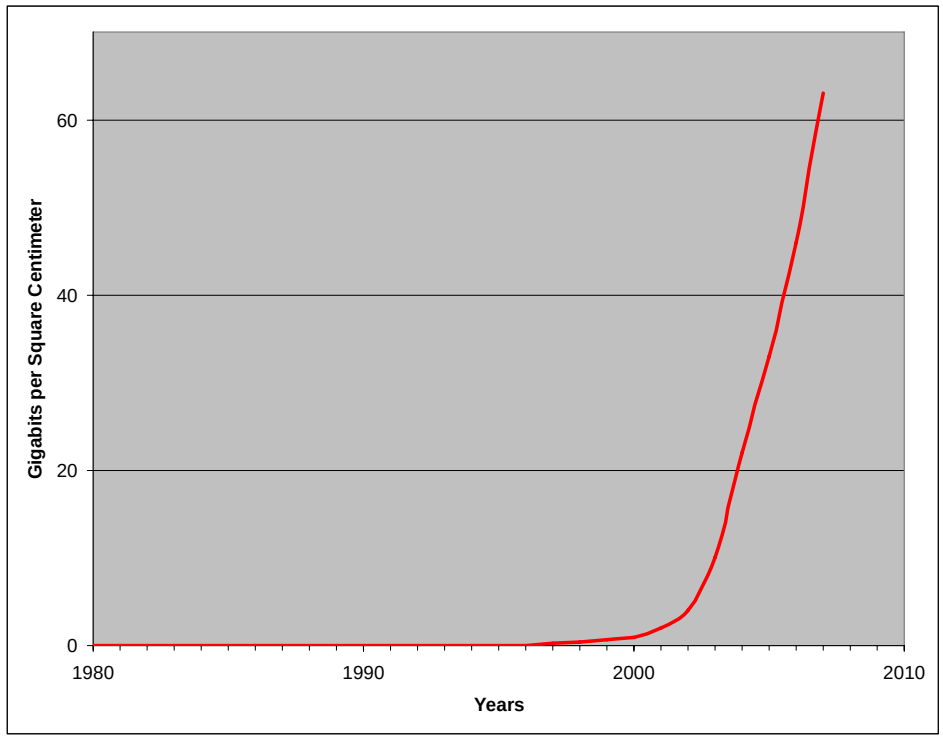
A Theory Will Serve to *Categorize* Intellectual Capital



- Recipients: **Cyber Policy Makers**
- Support: Operations Analysts
- "Wild cards": Futurists

A Theory Will Serve to *Explain*: Cyberspace (1 of 2)

- Cyberspace "rules of thumb"; e.g.,
  - Moore's Law (e.g., design of micro-electronics)
  - Proliferation of IP addresses (in transitioning from IPv4 to IPv6)
  - Increase in hard drive capacity (2007 Nobel Prize in Physics)



Introduction of Giant-Magnetoresistance Drives
(Gigabits/cm^2 vs. Time)

A Theory Will Serve to *Explain*: Cyberspace (2 of 2)

- Strawman "principles of conflict"
  - The offensive has the advantage; e.g.,
    - "Target rich" environment (difficult for defense to prioritize, defend selected targets)
    - Challenges of attribution
  - If cyberspace is to be more resistant to attack, it may require a new architecture that has "designed in" security
  - It will be a challenge to transition from the current legacy system to a more secure objective system

A Theory Will Serve to *Explain*: Cyberpower

- "Rules of Thumb" for Cyberpower
  - Regard "Metcalfe's Law" as a myth (i.e., "value" varies as N^2)
- Selected observations on military effectiveness
  - Studies of prior military theories (e.g., Mahan and Sea Power) have served to identify
    - Key factors of cyberpower
    - The need for risk assessments
  - In net-centric operations (NCO), the network helps, but it is not clear in what way
  - "I-Power" can be the basis for enhanced performance in Stability and Humanitarian Assistance/Disaster Relief (HA/DR) operations
- Selected observations on Information operations
  - Based on operational objectives, there is a need for changes in Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, and Facilities (DOTMLPF)
  - "New media" have the potential to revolutionize strategic communication

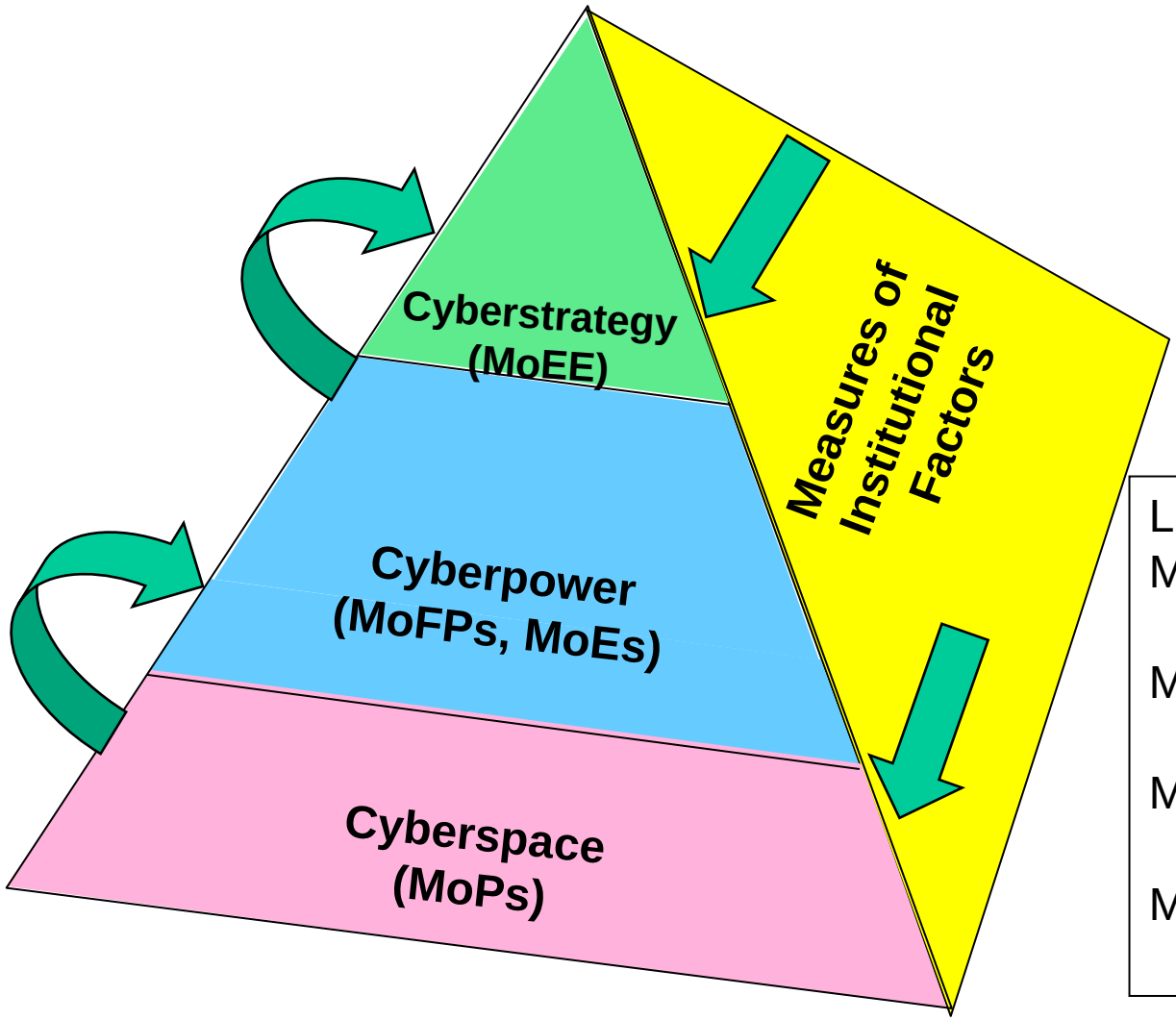
A Theory Will Serve to *Explain*: Cyberstrategy

- The “low end” users (e.g., individuals, hacktivists, terrorists, trans-national criminals) have enhanced their power considerably through recent cyberspace trends
- Potential near-peer adversaries are aggressively exploring options to exploit attributes of cyberspace (e.g., exfiltration of data; implementation of innovative cyber strategems)
- In light of the 2007 attack against Estonia, NATO is rethinking its cyber policy (e.g., Bucharest communique, creation of a Cyber Defense Management Authority)
- A theory of “cyber-deterrence” is beginning to emerge, drawing on all levers of power

A Theory Will Serve to *Explain*: Institutional Factors

- Given the complexity of the governance mechanisms, one should seek *influence* over cyberspace vice *governance*
- The legal community has barely addressed the key cyber issues that must be resolved during the next decade; e.g.,
  - What is an act of (cyber)war?
  - What is an appropriate response to a “cyber attack”?
- There is a need for a framework and enhanced dialogue between champions of civil liberties and proponents of enhanced cyber security to establish an adequate balance
- Guidance and procedures are required to address the issue of sharing of cyber information between the USG and industry

A Theory Will Serve to *Connect*



Legend:
MoPs: Measures of Performance
MoFPs: Measures of Functional Performance
MoEs: Measures of Effectiveness
MoEE: Measures of Entity Empowerment

A Theory Will Serve to *Anticipate*: Cyber Research Challenges

Area	Research Areas
Cyberspace	• Perform **technology projections** to identify key breakthroughs • Explore options to enhance **attribution** • Develop techniques to **protect essential data** from exfiltration, corruption • Formulate an **objective network architecture** that is more secure, and identify options to transition to it
Cyberpower	• Extend analyses to **other levers of power** (e.g., diplomatic, economic) • Perform **risk assessments** to address cyber-dependence • Quantify the Blue-Red **information duel**
Cyberstrategy	• Conduct research on **"tailored deterrence"** • Identify S&T to enhance **strategic communication** • Explore options to address **cyber espionage**
Institutional Factors	• Perform research on **cyber influence; legal frameworks; balance between security and civil liberties**
Cyber Assessment	• Develop analytical methods, tools, data, and intellectual capital **to assess cyber issues**

A Theory of Cyberpower: Residual Challenges

Area	Assessment	Residual Challenges
Define	Green-Amber	• Rationalize key definitions (e.g., cyber; domain; information operations)
Categorize	Green-Amber	• Develop a family of frameworks to address various policy issues
Explain	Green-Amber	• Address a variety of topics that have not been treated in the book (e.g., civil liberties; diplomatic, economic issues)
Connect	Red	• Develop appropriate Measures of Merit (MoMs) and explore their linkages
Anticipate	Red-Amber	• Improve assessments of highly non-linear trends

Summary

- The CTNSP Team has
  - Developed a preliminary theory of cyberpower
  - Generated a book on the subject that consists of approximately thirty chapters
  - Identified many key cyber policy issues and formulated preliminary recommendations
- However,
  - Considerable effort is required to enhance the evolving theory of cyber
  - Many of the key policy issues require additional analyses